



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/353,974	07/15/1999	VIKTORS BERSTIS	AT9-99-123	4395

7590

08/21/2003

DUKE W YEE
CARSTENS YEE & CAHOON LLP
P O BOX 802334
DALLAS, TX 75380

EXAMINER

SHAH, NILESH R

ART UNIT

PAPER NUMBER

2127

DATE MAILED: 08/21/2003

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/353,974

Applicant(s)

BERSTIS ET AL.

Examiner

Nilesh R Shah

Art Unit

2127

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 30 June 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 October 1999 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other:

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on 6-30-03.
2. Objections to the specification and claims have been withdrawn.
3. 35 U.S.C. 112 2nd paragraph rejections have been withdrawn.
4. Applicant's arguments filed on 6-30-03 have been fully considered but they are not persuasive.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 2, 4, 5, 10 - 12, 14, 15, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banga et al (5,931,904) 'Method for reducing the delay between the time a data page is requested and the time the data page is displayed' in view of Cuccia et al (6,151,676) 'Administration and utilization of secret fresh random numbers in a networked environment.'

7. As per claims 1, 2, 5, 11, 12, 15, 21 Banga teaches the use of a remotely located cache storage site 151. A session is initiated and the user 11 requests a page. The web site is received

by user 11 and then cached by the remote proxy 151 (col 3 lines 29-65). Banga also teaches that the cache data can be stored at a remote site (element 151 and col 3 lines 29-45).

The applicant argues that the cited references do not **‘describe encryption and caching of a received web page’**. In view of this remark, what is disclosed by Banga is the receiving of a web page and storing a particular version of a cached page at a remote site. Arguments are found to be non- pervasive. (col. 3 lines 29-65) (‘First, the remote proxy must cache at least one version of the page (if the page requested by the user has never been requested by any user connected to the remote proxy, there would be no alternative to waiting for the full current page to be received at the remote proxy and sending the entire page, except that it may be possible to begin sending the entire current page before it is completely received at the remote proxy).’) Banga does not teach the use of encrypting the web page.

Cuccia teaches the use of a browser supported encryption algorithm. Cuccia teaches that the El-Gamal is an encryption algorithm, which is supported by a browser (col 6 lines 13-29). Cuccia teaches that the El-Gamal algorithm encrypts the data (web page) to ensure the integrity of the data (col 5 lines 4-61, col 8 lines 13-37). This technology, which uses public key encryption, is incorporated into the web browser. Also it discloses on selecting the browser which is supported by El-Gamal (col 6 lines 13-29).

Applicant argues that the reference do not teach **‘encrypting a web page’** in view of this, what is disclosed by Cuccia clearly suggests the encryption of a web page. Arguments are found to be non- pervasive. (col. 5 lines 4-61, col. 8 lines 13-37) (‘The operation of the networked system 10 in providing a secret fresh random number R1 and encrypted private key KprUser to the user in

Art Unit: 2127

the course of a phase in the nature of a challenge response protocol, which after completion of this phase, are used for a digital signature employing the El-Gamal algorithm of a document $S[K_{prUser}, R1](H(DOC))$ which is derived from, or the same as, a then supplied document, will be best understood by also referring to FIG. 2.) ('For the purposes of this Figure, it is assumed that the user has already requested access to the document system (home page) and the server 16 has sent a sign-in page to the user equipment 12. Thereafter at step 30, the user enters his ID in the sign-in page via input means 12a, e.g. the initials of the user, providing the IDs of all users are unique, and at step 40 the sign-in page including the entered ID is transmitted to the server, which receives it at step 70.') The use of encrypted private keys and the El-Gamal algorithm on the document (web page) is clearly shown by Cuccia. **In addition on page 16 of arguments applicant states certain limitations are not meant by references HOWEVER these limitations are not stated in the claims. Arguments are found to be non- pervasive.**

Therefore the Banga/Cuccia combination would disclose encrypting the web page and coding the web page using a browser supported encryption algorithm. It would be obvious to one skilled in the art to add the art to add the use of the El-Gamal algorithm to Banga to ensure documents (web page) are secure (col 1 lines 14-62). For this reason as well as the reasons stated above the combination of Banga and Cuccia clearly meet the limitations of the claims therein. Claims 1, 2, 5, 11, 12, 15, 21 are rejected.

8. As per claims 4 and 14 Banga teaches a session is initiated and the user 11 requests a page. The web site is received by user 11 and then cached by the remote proxy 151 (col 3 lines

29-65). Banga does not teach the use of encrypting the web page using an algorithm supported by a browser.

Cuccia teaches the use of a browser supported encryption algorithm. Cuccia teaches that the El-Gamal is an encryption algorithm, which is supported by a browser (col 6 lines 13-29). Cuccia teaches that the El-Gamal algorithm encrypts the data (web page) to ensure the integrity of the data (col 5 lines 4-61, col 8 lines 13-37). This technology, which uses public key encryption, is incorporated into the web browser. Also it discloses selecting the browser which is supported by El-Gamal (col 6 lines 13-29). Therefore the Banga/Cuccia combination would disclose encrypting the web page and coding the web page using a browser supported encryption algorithm. It would be obvious to one skilled in the art to add the use of the El-Gamal algorithm to Banga to ensure documents (web page) are secure (col 1 lines 14-62). Claims 4 and 14 are rejected.

9. As per claims 10 and 20 Banga teaches the use of a remotely located cache storage site 151. A session is initiated and the user 11 requests a page. The web site is received by user 11 and then cached by the remote proxy 151 (col 3 lines 29-65). The data is checked to make sure it is the same as the requested data (col 3 lines 36-65). Banga does not teach the use of encrypting/decrypting the web page.

Cuccia teaches the use of a browser supported encryption algorithm. Cuccia teaches that the El-Gamal is an encryption algorithm, which is supported by a browser (col 6 lines 13-29). Cuccia teaches that the El-Gamal algorithm encrypts the data (web page) to ensure the integrity of the data (col 5 lines 4-61, col 8 lines 13-37). This technology, which uses public key encryption, is incorporated into the web browser. Also it discloses selecting the browser which is

supported by El-Gamal (col 6 lines 13-29). It would be obvious to one skilled in the art to add the art to add the use of the El-Gamal algorithm to Banga to ensure documents (web page) are secure (col 1 lines 14-62). Therefore the Banga/Cuccia combination would disclose encrypting and decrypting data associated with the browser. Thus claims 10 and 20 are rejected.

10. Claims 3 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banga et al (5,931,904) 'Method for reducing the delay between the time a data page is requested and the time the data page is displayed' in view of Newton's telecom dictionary.

As per claims 3 and 13 Banga teaches the use of a remotely located cache storage site 151. A session is initiated and the user 11 requests a page. The web site is received by user 11 and then cached by the remote proxy 151 (col 3 lines 29-65). Banga also teaches that the cache data can be stored at a remote site (element 151 and col 3 lines 29-45). Banga does not teach the use of encryption algorithm that is not supported by a browser.

Newton's telecom dictionary also teaches the use of an encryption algorithm that is not supported by a browser. Kerberos is defined as a network authentication protocol, it is a UNIX-based distributed databases used for user authentication (page 423). Since authentication or preventing unauthorized users from accessing certain locations is form of encryption and a UNIX based database is not supported by a browser. The type of encryption application would change from the EL-GAMAL rejection in claim 1 to a Kerberos encryption algorithm which is not supported by a browser. Therefore the Banga/ Kerberos combination would disclose encrypting the web page and coding the web page using non-browser supported encryption algorithm. Claims 3 and 13 are rejected.

11. Claims 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banga and Cuccia as applied to claim 1 above, and further in view of Sadovsky (5,689,638) 'Method for providing access to independent network resources by establishing connection using an application programming interface function call without prompting the user for authentication data'.

As per claims 6 and 16 Banga teaches the use of a remotely located cache storage site and Cuccia teaches the use of encrypting the web page (see claim 1 rejection). Cuccia and Banga do not teach the use of a password associate with the cache.

Sadovsky teaches the use of password used to gain access to secure network resources (col 4 lines 42 –54). It would be obvious to one skilled in the art to add the password to the teachings of Cuccia and Banga to ensure that only authorized personal are able to view the cached data. Cached data is very sensitive resource thus as Sadovsky teaches it is very important to have a password because ' this form of security is essential in computer networks to prevent unwanted access to a computer network' (col 1 line 58-62). Claims 6 and 16 are rejected.

12. Claims 7 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Banga and Cuccia as applied to claim 1 above, and further in view of Billington et al (5,963,884) 'Predictive Maintenance System'.

As per claims 7 and 17 Banga teaches the storing of cached data on a remote site. Cuccia teaches the use of encrypting data. Banga and Cuccia do not specify the path for the memory location that stores the cached data.

Billington teaches that a specific path is used to store data (col 15 lines 34-40). Billington stores this data in-site or off-site and insists that different paths should be used for each system. It would be obvious to one skilled in the art to add the specific path of Billington to Banga and Cuccia to ensure that the exact location is secure and known. Claims 7 and 17 are rejected

13. Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cuccia and Banga as applied to claim 1 above, and further in view of Olson et al (4,847,758) 'Main memory access in a microprocessor system with a cache memory'

14. As per claims 8 and 18, Banga teaches the use of a remotely located cache storage site and Cuccia teaches the use of encrypting the web page (see claim 1 rejection). Cuccia and Banga do not teach the use of paged memory.

Olson teaches the use of storing the web page cache in a paged manner (col 4 lines 46-56).). ('By allowing the cache memory 16 to access the main memories 18 in a paged manner, cache memory efficiency, i.e., the hit ratio or the percentage of time that the required data is located in the cache memory, is improved allowing the data processing system 11 to operate substantially at the speed of the fast cache memory as disclosed and claimed in the co-pending application assigned to the assignee of the present application and cross-referenced above').

The applicant argues the lack of motivation to combine the reference Olson to Cuccia and Banga, Arguments are found to be non- pervasive. It would be obvious to add the paged memory to the teachings of Cuccia and Banga to improve the data processing system of the

remote proxy 151. in addition by using the page manner the remote proxy 151 can operate at a higher speed (col 4 line 48-56.) **The applicant argues that the process of encrypting the cache data would slow down the access speed but the data has already been encrypted before entering the cached area. Thus Arguments are found to be non- pervasive.** Claims 8 and 18 are rejected.

15. Claims 9 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schrader et al (5,903,881) 'Personal online banking with integrated online statement and checkbook user interface' in view of Banga.

As per claims 9 and 19, Schrader teaches the use of opening and using an application with a browser (col 13 lines 45-60). An application specific function such as making a payment to a specific person is done by using the browser (Fig 9). The browser opens a application specific (payment method) function that the user selects (col 8 line 25-51). After the payment is selected specific information is produced based on the application chosen such as amount and pay to information (figure 9, col 11 lines 40-67). The application specific information is encrypted (col 17 line 12-30). Schrader does not teach the use of caching the application specific information.

Banga teaches the use of a remotely located cache storage site 151. The web site is received by user 11 and then cached by the remote proxy 151 (col 3 lines 29-65). Banga also teaches that the cache data can be stored at a specific location (element 151 and col 3 lines 29-45). The specific web browser's creates the cached data. It would be obvious to one skilled in the art to add the

teachings of Banga to Schrader to ensure that the encrypted application information is cached.

By using caching application specific information the amount of time needed to load a page will be reduced (col 1 lines 7-49).

As per the arguments made by the applicant the about claims 9 and 19, Arguments are found to be non- pervasive. Schrader teaches the use of encrypting application specific information (col. 17 lines 12-30) ('To provide security, the personal online finance application 304 provides for user authentication during banking transactions, and file encryption of transmitted data and instructions. The request file is preferably encrypted using RSA.TM. 1024 bit triple DES encryption. The request file is encrypted with the public key of the receiving financial institution, and then transmitted to the financial institution computer system 305.'). **The examiner states in the previous action that Schrader does not teach the storing of cache information. Further Bange teaches the use of a remotely located cache storage site for data (col. 3 lines 29-65).** It would be obvious to one skilled in the art to add the teachings of Banga to Schrader to ensure that the encrypted application information is cached. By using caching application specific information the amount of time needed to load a page will be reduced (col 1 lines 7-49). 'The cache memory provides a buffer storage for the portion of the main memory that is currently being used. It also contains a translation of the main memory address into this buffer storage. For this reason, cache memories are said to have "temporal" locality. This is a primary benefit of cache memories since previous data processing system studies have shown that operating programs generally exhibit a great deal of temporal locality.')

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nilesh R Shah whose telephone number is 703-305-8105. The examiner can normally be reached on Monday-Friday 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Grant can be reached on 703-3058-1108. The fax phone numbers for the organization where this application or proceeding is assigned are (703)305-0040 for regular communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Application/Control Number: 09/353,974
Art Unit: 2127

Page 12

NS
August 13, 2003


MAJIDA A. BANANKHAH
PRIMARY EXAMINER